TEXT MESSAGING ENCRYPTION SYSTEM

NIRMALA DEVI A/P SUNDARA MORTHTHY

A thesis submitted in partially fulfillment of the requirements for the award of degree of
Bachelor of Computer Science (Networking Engineering)

Faculty of Computer System & Software Engineering
University Malaysia Pahang (UMP)

JUN 2012

ABSTRACT

Text Messaging Encryption system is a text message encryption and decryption. Encryption is a process of masking a message so that it is unreadable. Encryption is important to avoid other people to read certain information. The only way to read the information is to know the method on how message is being masked, in this case knowing the algorithm used to encrypt the message. Nowadays, most encryption and decryption processes are done by the computer. The main objective of this project is to build a text encryption and decryption system that will run on a Java enabled mobile phones. Then, the mobile phones will be used as an external means to encrypt text messages. As mentioned earlier, not only computers can encrypt and decrypt text but mobile phones also can encrypt and decrypt text messages. The purpose of this research is to provide security for confidential information to be sent over mobile phones. At the moment there is no security for messages transmitted over mobile phones. Confidential information or instructions can only be safely passed on to the required parties by email or verbally in person. This delays time and efficiency of crucial business operations. Currently messages in phone can easily be read if the phone is stolen, or users might simply send it to the wrong number. Messages need to be encrypted to solve this problem. With this only the sender and recipient will be able to send and receive private information. At present, banking, commerce and passwords can only be communicated with internet connection or as in person verbally or in written; Text Messaging Encryption system needs to overcome this intermediate subjects and deliver instructions or messages instantaneously and securely. The programming language that is used to write the program is Java Language.

ABSTRAK

Sistem Enkripsi Pesanan Ringkas adalah sistem yang merujuk kepada penyulitan dan penyahsulitan mesej. Enkripsi ialah satu proses masking mesej supaya mesej itu tidak boleh dibaca oleh orang lain. Satu-satunya cara untuk membaca informasi itu adalah dengan mengetahui kaedah yang digunakan untuk masking mesej tersebut, dalam kes ini caranya adalah dengan mengetahui algoritma yang digunakan untuk menyulitkan mesej tersebut. Pada masa kini, kebanyakan penyulitan dan penyahsulitan mesej boleh dilakukan daripada komputer. Objektif utama projek ini adalah untuk membina satu sistem yang boleh berjalan dalam telefon bimbit yang meyokong bahasa Java. Selepas itu, telefon bimbit itu akan digunakan sebagai cara luar untuk penyulitan mesej. Seperti yang diberitahu awal lagi, bukan sahaja computer boleh menyulit dan menyahsulit mesej tetapi telefon bimbit pun boleh. Tujuan utama penyelidikan ini adalah untuk meyediakan sekuriti untuk maklumat sulit dihantar melalui telefon bimbit. Pada masa kini, tiada sekuriti disediakan untuk mesej yang dihantar melalui telefon bimbit. Maklumat sulit atau arahan boleh dihantar dengan selamat kepada orang yang memerlukan melalui email atau bercakap terus kepada orang tersebut. Ini boleh melengahkan masa dalam operasi perniagaan. Pada masa ini, mesej dalam telefon bimbit boleh dibaca dengan senang jika telefon bimbit telah dicuri, ataupun pengguna mungkin tersalah hantar kepada nombor yang salah. Mesej perlulah disulitkan untuk mengatasi masalah. Sekarang, dalam kaedah banking kata laluan hanya boleh berkomunikasi dengan sambungan internet atau bercakap terus atau dengan menulis. Sistem Enkripsi Pesanan Ringkas perlu mengatasi masalh ini dengan meyampaikan arahan ataupun mesej dengan selamat. Bahasa pengaturcaraan yang digunakan untuk membuat sistem ini ialah bahasa Java.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

This chapter briefly describes the Text Messaging Encryption System that will be developed later. This chapter comprises five sections: The first section describes the background of the project. The second section describes the problem statement and motivation of the project. The third section describes the objectives for the project. The fourth section describes the scopes for the project. Finally the thesis organization is described in section five.

1.1. Background

Many times when data is exchanged electronically the privacy of the data is a requirement. The use of encryption restricts unintended recipients from viewing the data, which are deemed confidential and potentially dangerous if made known to irresponsible parties.

Today, encryption is the procedure of transforming plaintext, data that can be read by anyone, to cipher text, data that can only be read by someone with a secret decryption key. A message before being changed in any way is called plaintext. Plaintext messages are converted to cipher text via some encryption method. A particular such method is called a cryptosystem.

Encryption today is highly competitive businesses often require that extensive security measures be put into place. And, those who wish to exercise their personal freedom, outside of the oppressive nature of governments, may also wish to encrypt certain information to avoid legalities that entailed possession of such.

This final year project is concentrated on Text Messaging Encryption System. Currently SMS is being widely used as a fast and convenient communication tool. There is no age barrier in using this SMS service which starts from small kid till elderly people. When this is the case, there is no security for messages transmitted over hand phones on the required parties by email or verbally in person. This delays time and efficiency in crucial business operations.

Since there is no security for the messages, it indirectly leads to a lot of problems where important and confidential information such as passwords is being accessed by unauthorized individual. Apart from all that, there are also some other cases like the mobile phone owner accidently send messages to the wrong number and it gets worse when the mobile get stolen.

By implementing this encryption system, security of private and confidential data will be solved. This system is not only meant for public use but it is also focused on banking and commerce sectors as well where this system is more in need to basically interact with their customers. This system will be targeted to be very user friendly in where it will be very easy to handle and provides good security at the same time. Due to this reason, more people will get to know about the product and it is believed to be utilized in an appropriate way.

1.2.Problem Statement and Motivation

Although it is widely used, there is no security for messages transmit over hand phones at moment unless the users take their own initiative to install encryption software which is available in the market. As for now, not much people

realize the existence of encryption software's in the market. They do not know on how to really utilize it and how secure it as well. SMS encryption is required to provide security for confidential information to be sent over hand phones. Confidential information or instructions can only be safely passed on to the required parties by email or verbally in person. This delays time and efficiency of crucial business operations. Currently messages in phone can easily be read if the phone is stolen, or users might simply send and receive private information. At present, banking, commerce and passwords can only be communicated with internet connection or as in person verbally or in written. SMS helps to overcome this intermediate subjects and deliver instructions or messages instantaneously and securely.

After analyzing the above stated problem, this system will encrypt and decrypt the messages which are sent through mobile devices using GSM connection. This mobile application starts off with a login screen which requires the user to key in their respective username and password. The user will type the message in the encryption system which will then be then sent out to the intended recipient by entering their phone number. The recipient will receive the message in the form of cipher text which will be then copied to the system to decrypt it and get the original message back using the same SMS Encryption system installed in his/her mobile phone. Since the messages are being encrypted, it provides a good security system.

The system basically concentrates on providing 1st level of security for the text message content itself which can be private and confidential in so many situations as fraud cases based on this can be listed down. This is the part where the user will be able to encrypt and decrypt the messages from the developed system which protects their valuable data. Other than that this system would be providing security at initial point on 2nd level security which concentrates on user authentication. This is basically done to avoid unauthorized access if someone else attending the phone instead of the real user if the phone gets stolen. This is possible because only the

original user have the unique username and password which was registered earlier in the system.

1.3 Objective

There are few objectives which is concentrated throughout developing this Text Messaging encryption system:-

- To provide a proper security for SMS through encryption and decryption techniques with suitable algorithm which is targeted to prevent any fraud to take place in the case where communication of private and confidential data.
- To develop a system that is user friendly in where the system will be easy to handle and secure at the same time.
- To work the system as expected without any errors and reach the users so that they can adapt to its functionality by giving importance on the user requirements throughout the development process

1.4 Scope

There are few scopes implemented for this Text Messaging Encryption System which are as follows:-

- The system will concentrate mainly on encryption and decryption function for SMS.
- The system is for only Java enabled phones.
- This system is a standalone application.
- Both sender and recipient must have the software installed in their phones.

1.5 Thesis Organization

This thesis consists of five chapters. Chapter 1 will discuss the background of the study, problem statement, objective, and scope of study. The background of the study explains general information on text encryption. While the problem statement discusses the possible problems that need to be overcome throughout this project, the problem faced by sending private messages without secure and the effects . The main purpose and aim of this project is elaborated under objective. Scope of the study explains the characteristic of the system and some restrictions of the Text Messaging Encryption system. Chapter 2 will discuss about the related studies of Text Messaging Encryption System which is the literature review part. It also will discuss about the existing system that have similar function as the proposed system. Chapter 3 will discuss about the methodology of the system and also the characteristics of the system. Besides that, chapter 4 will discuss about the implementation and also testing that is carried out for this system to perform well. Finally, chapter 5 will conclude the whole chapters and also about the system. It also discusses about the limitations and future enhancement of Text Messaging Encryption system.

CHAPTER II

LITERATURE REVIEW

This chapter briefly describes the review on existing techniques related with Text Messaging Encryption System. This chapter comprises ten sections: The first section describes about the security concepts. The second section defines the encryption terms while the third section discusses about the history of encryption. The fourth section describes the comprehensive review on existing related systems. The fifth section describes the symmetric encryption and examples of its algorithms. The sixth section describes the asymmetric encryption and examples of its algorithms. The seventh section discusses about the characteristic of the project while the eighth section describes about the Java programming language. The ninth section discusses about the Netbean software. Finally, the tenth section will summarize the whole chapter.

2.0.1 What is computer security?

In the area of computer science, security is one of the prevention or protection against, access to information by unauthorized recipients, and intentional but unauthorized destruction or alteration of that information(Oxford: Oxford University Press, 1996).This can be re-stated: “Security is the ability of a system to protect information and system resources with respect to confidentiality and integrity." Note that the scope of this second definition includes system resources, which include CPUs, disks, and programs, in addition to information.

2.0.2 A Taxonomy of Computer Security

Computer security is normally associated with three core areas, which can be summarized by the acronym "CIA":

- **Confidentiality** – This will ensuring that information is not accessed by unauthorized persons
- **Integrity** – This will ensuring that information is not altered by unauthorized persons in a way that it is also not detectable by authorized users
- **Authentication** – This will ensuring that users are the persons they claim to be

A strong security protocol addresses all three of these areas. For an example, Netscape's SSL (Secure Sockets Layer) protocol. It has enabled an explosion in ecommerce which is really about trust (or more precisely, about the lack of trust). SSL overcomes the lack of trust between transacting parties by ensuring confidentiality through encryption, integrity through checksums, and authentication via server certificates.

Computer security is not restricted to these three broad concepts. Additional ideas that are often considered part of the taxonomy of computer security include:

Access control – This will ensures that users access only those resources and services that they are entitled to access and that qualified users are not denied access to services that they legitimately expect to receive

Nonrepudiation – This may ensures that the originators of messages cannot deny that they in fact sent the messages (New York: Simon and Schuster, 1997).

Availability – This ensures that a system is operational and functional at a given moment, usually provided through redundancy; loss of availability is often referred to as "denial-of-service"

Privacy – It will ensuring that individuals maintain the right to control what information is collected about them, how it is used, who has used it, who maintains it, and what purpose it is used for

These additional elements do not neatly integrate into a singular definition. From one perspective, the concepts of privacy, confidentiality, and security are quite distinct and possess different attributes. Privacy is the property of individuals; confidentiality is the property of data; and security is the property assigned to computer hardware and software systems. From a practical perspective, the concepts are interwoven. A system that does not maintain data confidentiality or individual privacy could be theoretically or even mathematically "secure," but it probably wouldn't be wise to deploy anywhere in the real world.

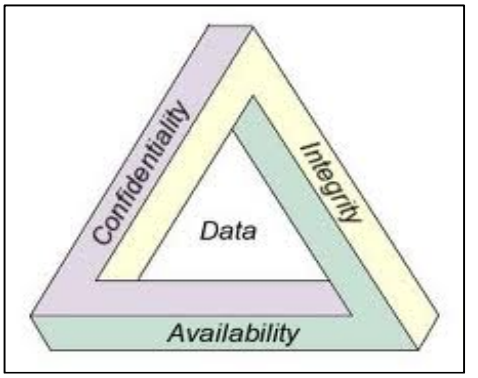

Figure 2.1: Taxonomy in security

2.1 Definition of Encryption

Encryption is a famous security method which is used to secure text messages and other related essential data's. The encrypted messages will be in the form of unreadable and not meaningful text that only can be decrypted using the appropriate key which acts between the sender and the recipient. A good and secure encryption can only be developed with an appropriate and intricate algorithm which will make it complicated for unauthorized person to break it.

Encryption works with many different types of algorithms which is available. Each algorithm has its own advantages and disadvantages. This algorithm is the most important element in an encryption system which is responsible to change the

original content of data or text and finally decode it back. This algorithms works with a unique key assigned to it which acts in between plain text and cipher text. Without the key, it is impossible for anyone to decrypt to its original content.

"The most popular use of encryption is for securing web servers that are accessed by the https protocol not http so that data such as credit cards can be sent safely over the internet." (David Bolton)

There are two types of encryption which is symmetric and asymmetric encryption. Symmetric encryption is also known as private key encryption while asymmetric encryption is also known as public key encryption. Example of private key encryption is Data Encryption System (DES), Advanced Encryption Standard (AES) and RC4. As for the public key encryption, the example is RSA, DSA and PGP. [1]

2.2 History of Encryption

Encryption was there long way back and it was introduced since the need for privacy has always been there. Besides that, it plays an important role in securing private and confidential information to be passed on.

One of the first "unbreakable" codes was Mary's Queen of Scots. This code was initiated for the purpose of communication but then it was broken into which then led to her conviction and execution.

After that, it was the turn of Blaise de Vigenere to publish Traicte des Chiffres describing a new cipher, Le Chiffre Indechiffrable (The Indecipherable Cipher) which was reliable for almost three centuries and finally this code also become victim of code breakers.

The next code which came to acceptance was the Beale Cipher. This was implemented to encrypt papers that describe the whereabouts of treasure buried in the 1819 and 1821. One of the keys that are used for this cipher was the Declaration

of Independence. End of the day, since the rest of the keys could not be found by anyone, nobody manage to find the treasure yet.

Now, it is time to discuss about encryption codes which made name during the First and Second World Wars or should it be mentioned as hard times. Securing the communication became even vital when it comes to war times. This is where the starting point of United States' Navajo Code which was not broken during the war and there was

Other than all the above mentioned, encryption was focused on something different which was "cracking" ancient languages. In this effort, the first decryption that took place was Egyptian hieroglyphs. This is done using Rosetta stone which is believed to be an artifact that had the same messages written in three languages. Besides that, after a continuous effort through cryptanalysts, another ancient language was deciphered which is quite well known, Mediterranean language.

The modern encryption methods are focused by using the latest technologies which is mostly with the aid of computers. The algorithms used these days are more advanced compared to last time to cater the security need as electronic transmission are widely being used these days. [2]

2.3 Existing software

2.3.1 WMkits SMS Encryption

WMkits SMS Encryption is professional text messages encryption software for Windows Mobile phones. It can encrypt and hide the SMS messages (including existing SMS messages and future incoming/outgoing SMS messages) on the windows mobile devices. The hidden SMS messages are encrypted and will be stored separately. You can only decrypt and show your messages with a correct password. That means, others cannot view any of your secret or important SMS messages on your mobile phone without your approval, even if you lost your phone

or lend your mobile phone to your friend or relative. Your privacy will be safe. [20]

Key features:

- It encrypts and hide all existing SMS on your file folders, including SMS default folders (Inbox, Outbox, Drafts, Deleted, Sent) and custom folders.
- It can encrypt and hide future incoming SMS and outgoing SMS in real time.
- There are multiple encryption modes available. By settings, you can choose to encrypt sent SMS, received SMS, SMS from/to your wanted contact(s) or all SMS.
- It will be using AES 128-bit encryption. Passwords will be private, encrypted and saved.
- It is a powerful SMS management. WMkits SMS Encryption supports threading mode of your encrypted messages and Page Views. Besides, you can use it to directly reply, copy, forward or delete SMS exactly the same as on your phone.
- It is safe and easy to decrypt SMS. You can choose to decrypt your SMS by settings.
- This able to decrypt and transfer SMS onto your new windows mobile phone. It has a large memory for SMS. SMS backup and restore functions supported. We no need to worry about any loss of your encrypted SMS.
- The login password and encrypted SMS are keeping safely even if you uninstall this software.
- It is easy and safe to install/uninstall.
- It is simple and have intuitive interface.
- It is compatible for all windows mobile (Pocket PC) phones.

System Requirements

Windows Mobile 5, Windows Mobile 6

Table 2.1: Advantages and disadvantages of WMKits SMS Encryption

ADVANTAGES	DISADVANTAGES
It can encrypt and hide the **SMS** messages (including existing **SMS** messages and future incoming/outgoing **SMS** messages) on the windows **mobile** device.	The encoded image can be saved only as a bitmap file.
The hidden **SMS** messages are encrypted and stored separately.	
Only the owner can decrypt and show his/her messages with a correct password. That means, others are not able to view any of his/her secret or important **SMS** messages on his/her **mobile** phone without their approval, even if they lost your phone or lend it to their friend or relative.	

2.3.2 Secure SMS

Secure SMS is a simple to use, but extremely sophisticated software that provides you with complete security when sending and receiving SMS text messages. Secure SMS solution is ideal for both individuals and businesses that care about their privacy. Secure SMS fully protects you from commercial espionage, governments, mobile phone companies, and any third parties (using GSM interception systems) who seek to discover any sensitive information or private correspondence.

In short Secure SMS is your one-stop-shop for sending and receiving all your text messages in complete confidence that you are the sole recipient. All your text messages transferred over the GSM or CDMA networks will be encrypted (end to end encryption).